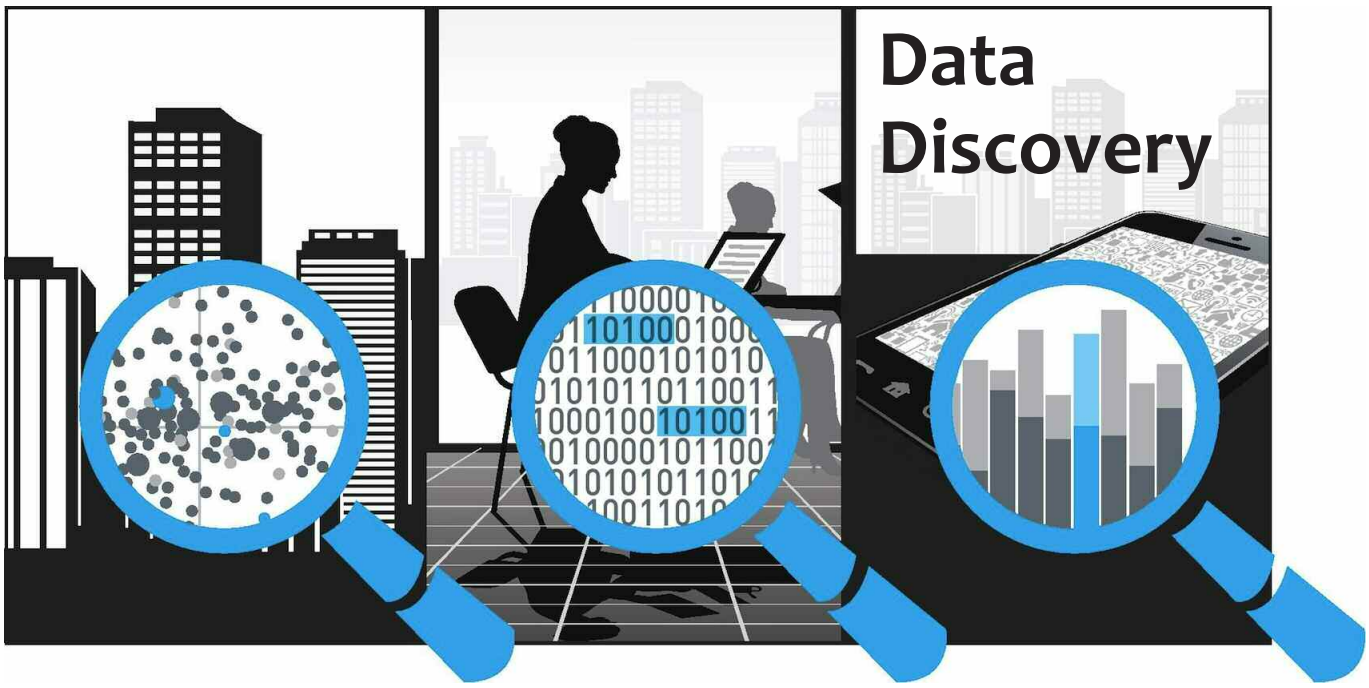


Mobile phones and other digital devices may be concealing a wealth of intelligence that could alter the course of an investigation but often remain hidden according to Simon Lang, Digital Forensics Manager at SYTECH.

It is now a well-established fact that mobile phone evidence plays an integral part in the evidential process in today's criminal investigations. Looking back over the past decade, who could have imagined the major role that technology – in particular mobile phones would play in our lives and in the lives of criminals.

Even though mobile phone evidence is common place, there is still a wealth of intelligence contained on handsets that investigators could still be missing. This is because of the misconception that all you need to do is plug a mobile phone into a device and extract the data.

What is key is not just the data you extract but how you apply an investigative mind set to analyse that data, translate it into intelligence and then assess where it could potentially lead an inquiry.

Our approach at SYTECH is to start from the premise that every mobile phone contains a wealth of hidden data that could prove vital to an investigation. While I accept that the increase in the role of mobile phones in investigations has led to a back log in forces and that money is finite – this should be weighed up against the evidential potential that might be being ignored that could have a big impact on the outcome of a case.

One of the current myths I have heard is that data can't be extracted and analysed from PIN or Password protected Blackberry devices. It's also a myth that if a Blackberry is sent away to companies such as ours then it will take weeks to recover the evidence. We have become experts at analysing locked Blackberry devices and are capable of turning jobs around in a day if required utilising some of the most advanced examination methods in the area of Digital Forensics.

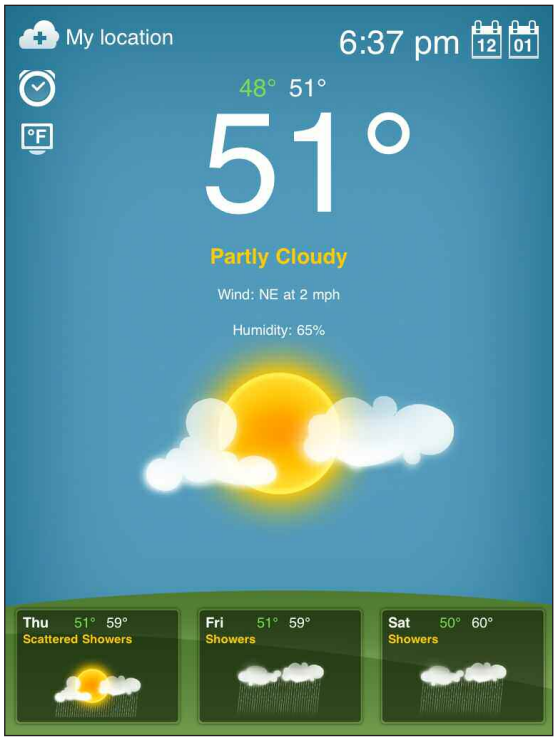
We have recently made a game changing breakthrough with the newer generations of PIN or Password protected Apple iPhone and iPad devices.

Even if the devices are locked, as with the previous iterations of Apple Handsets SYTECH are able to gain access to this crucial evidential data held within the newer iPhone 4S, iPhone 5, iPhone 5S, iPhone 5C Handsets and iPad devices which up until now have not been possible.

Mobile Applications

In the ever-changing and evolving world of technology, there are also a number of features on phones such as Apps and messaging services that could potentially be concealing vital information. Free APPs such as Snapchat, WhatsApp and BBM are often used as a free way of texting and the myth is that the data is not as easy to recover as conventional texts.

As these messaging services are free, more and more people – including criminals are using them as a way of communicating without thinking that the data could be recovered. We constantly keep up-to-date with all the latest messaging Apps and can extract valuable data from them all which can then be analysed in the same way as text messages.



We have even used a hidden data within a weather App to confirm the location of a suspect who claimed he had been elsewhere at the time of a crime. As weather Apps rely on GPS and Timing data then it's easy to track down towns, post codes and exact co-ordinates to prove a person's location.

I'm sad to say that Snapchat and other messaging APPs are also increasingly being used to send indecent images, again because people are under the misapprehension that the data won't be traceable.

Simon Lang

As the pace of technological advancement is gathering pace by the day, my team and I liken it to a game of cat and mouse where we have to remain one step ahead of the criminal by researching all the latest developments, mobile security, new Apps and services that are being brought out almost daily. We are really passionate about what we do and see it as more of a vocation than a job and so we consider it vital to be ahead of the game in terms of technological advancement.

Future

Looking to the future, issues around encrypted phones and cloud storage will continue to be a challenge and are issues that we are determined to address and try and find solutions for. Some the new mobile phone handsets are encrypted by default therefore it makes it difficult to extract data from, but not impossible. Currently the main issue with cloud storage is who actually has jurisdiction of the databases online?

We see our roles of external consultants as working alongside investigation teams from the outset, not just analysing the phone but also providing on-going input that continues to the court room where we give evidence as expert witnesses on a monthly basis.

While we acknowledge that the future is uncertain in the world of technology, what is certain is that we always try and stay one step ahead – and that's no easy task.

For more information on SYTECH go to: www.sytech-consultants.com or email enquiries@sytech-consultants.com